**Testimony of**
**Joseph M. Weiss**
**Control Systems Cyber Security Expert**

**before the**

**House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census**
**U.S. House of Representatives**

**March 30, 2004**

# Control Systems Cyber Security—Maintaining the Reliability of the Critical Infrastructure

**Joseph M. Weiss, PE, CISM**
**Executive Consultant, KEMA, Inc.**

Good afternoon Mr. Chairman, Ranking Member Clay and Members of the Committee. I would like to thank the Subcommittee for your commitment to a comprehensive examination of the cyber security of the control systems of our nation's critical infrastructure. I also want to thank you for the opportunity to be here today to discuss this very important topic with you.

My remarks will provide details on:
(1) Control systems design considerations and cultural issues;
(2) Control systems cyber vulnerabilities, and
(3) Key activities that need to be addressed and funded to secure control systems.

On July 24, 2002, I testified to Congressman Steven Horn's Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. At that time I stated that since September 11, 2001, the focus of security in the United States has been on physical terrorist attacks. Cyber security focus has been directed towards Internet use and networking technology. Dramatic steps are being taken to ensure security against physical attacks and increased emphasis is being placed on securing the Internet and networking systems for traditional IT business systems.

However, the same cannot be said for operational control systems, which are at the heart of our critical infrastructures and endemic across many industries. Control systems include distributed control systems (DCS) and programmable logic controllers (PLC) – also referred to as process control systems (PCS) - and supervisory control and data acquisition (SCADA) systems. These systems are crucial to the operations of, and form the backbone of, the global industrial infrastructures. The industrial infrastructures include electric power, oil and gas, chemicals, pharmaceuticals, water, paper, metal refining, auto manufacturing, transportation, and food processing to name a few.

It is important to note that there are a limited number of operational control systems suppliers, and the same systems are sold virtually in every country throughout the world.

There is a growing threat of cyber attacks on operational control systems that could create a crisis for which no country, company, or person is adequately prepared. Based on my knowledge of, and experience with, control systems I believe this is a very real possibility. I will provide several recommendations on how the government can help secure our nation's critical infrastructures from intentional and unintentional cyber events.

I am involved in a number of organizations and activities that have provided me insight, expertise, and a working knowledge of the cyber security issues we face as a nation and as a world community. I am a member of many active groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council 's (NERC) Critical Infrastructure Protection Committee (CIPC), ISA's SP99 Manufacturing and Control Systems Security Committee, and the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF). I would like to state for the record that the views expressed in this testimony are mine. I am not representing any of the groups in which I am involved.

I also would like to add that representatives from the following organizations have reviewed this document: Department Of Energy's (DOE) Office of Energy Assurance and National Energy Technology Laboratory, Department of Homeland Security's Cyber Security and Protective Security Divisions, Idaho National Engineering and Environmental Laboratory, Sandia National Laboratory, Government Accounting Office, Carnegie-Melon's Software Engineering Institute (CERT/CC), United Telecom Council, and a utility member of the NERC CIPC.

## Abstract

Control systems have been designed to be efficient, rather than secure. These systems are used throughout the industrial infrastructure. To date, there have been more than forty cases where control systems have been impacted by electronic means. These impacts have included damage to systems and the environment.

In order to better secure the control systems controlling the critical infrastructures there is a need for the government to support industry in two critical areas:

- ***Establish an industry-wide information collection and analysis center for control systems modeled after CERT*** (Computer Emergency Response Team) to provide information and awareness of control systems vulnerabilities to users and industry. There are existing mechanisms that can be adapted to support this type of activity such as Carnegie-Melon University and KEMA's activities within the CERT/CC and others.

- ***Provide sufficient funding for the National SCADA Test Bed*** to facilitate the timely and adequate determination of the actual vulnerabilities of the various control systems available in the market and develop appropriate mitigation measures.

## Control Systems Design Considerations

***Control systems were originally designed to be isolated***. - Control systems are used throughout all industrial manufacturing, utility operations and management, transportation, and other critical infrastructure sectors. Control systems are unique in their design and are directed to perform specialized tasks. They were originally designed to be isolated - that is, separate from other corporate enterprise computing. Unfortunately from a security perspective, competitive pressures have forced businesses to interconnect office and electronic commerce systems with these control systems. This has inadvertently exposed control systems directly to the Internet, intranets, and remote dial-up capabilities that are vulnerable to cyber intrusions.

***The control systems industry and its users are not well positioned to utilize security technologies as they are being developed and implemented in traditional business IT applications.*** - Control systems are designed with digital processors that have limited computing resources that are specifically designed, implemented, and embedded into their various process control equipment. Control systems are ubiquitous throughout many industries and are expected to have long-term use (more than 5 to 10 years) before replacement is necessitated. Unlike traditional business systems, control systems are not typically replaced when a faster, more powerful processor or new operating systems release is developed. Control systems are replaced when the system becomes obsolete, cannot be supported for lack of parts, or can no longer support functional requirements. Consequently, the control systems industry and its users are not well positioned to utilize security technologies as they are being developed and implemented in traditional business IT applications. Further, economic pressure dictates that minimal upgrade and improvement funding is available in today's competitive environment.

***Control systems design constraints preclude use of existing security technology***. - Control systems are deterministic in their design and operation. That means these systems have been designed with critical timing requirements, rigid performance specifications, and specific task priorities. These systems are also computer-resource and communication bandwidth limited. These constraints preclude use of existing security technology such as NIST-approved block encryption and Public Key Infrastructure (PKI). Block encryption and PKI are too resource intensive for many legacy control systems and may actually cause the systems to fail as they attempt to keep up with the intensive demands on their limited resources.

***Control systems communications utilize industry-accepted protocols that were designed without security considerations.*** - Many installations believe that having a firewall around the control system is sufficient. Firewalls may be one part of the security solution, but firewalls can be configured to be very restrictive or configured to be open. Unfortunately, my experience has shown that firewalls for control systems are not always configured effectively. Further, they are designed to filter Internet Protocols (IP) and were not designed to filter communication protocols used for control systems communication. Attempting to filter control systems protocols will require utilization of additional protective devices that may result in either unacceptable performance delays or require that control system information must be communicated without any filtering.

## Control Systems Culture Issues

What I am describing is a multi-fold cultural and technology gap that needs to be overcome. In most organizations information technology (IT) departments are responsible for cyber security. IT is traditionally well versed in cyber security for the commercial applications and have funding, although not necessarily sufficient funding to address all threats. IT also frequently reports through an organization's Chief Information Officer (CIO) to the executive board. However, IT typically does not have responsibility or accountability for the control systems that are a major component of their business and our critical infrastructure. On the other hand, an organization's operations-focused department is usually responsible for the control systems, but is typically not well versed in cyber security and often has little or no funding for cyber security.

There is often animosity between IT and operations. IT is perceived as not understanding what it means to maintain a system that has a greater than 99.99 percent reliability requirement and that must be available around the clock. As a point of illustration of this dichotomy, a two-level security solution that IT often proposes includes the requirement to add an additional password login function. This requirement might prevent a substation or power plant engineer from addressing a real-time outage or incident while attempting to get past a password lockout.

Another example of the IT-operations culture problem is that field engineering and maintenance personnel have, as their primary obligation, a duty to keep facilities operating. That obligation often translates into establishing remote dial-up or Internet connections to remotely access the control system to quickly diagnose existing problems. Unfortunately, this capability is sometimes implemented in a manner that is unknown to IT or to Central Engineering. Many of the system components share both phone lines and high-speed internal intranet connections - a significant, yet undocumented backdoor to the control systems.

Another concern is the use of non-control systems engineers to analyze the cyber vulnerabilities of control systems. Control systems have unique requirements that are uncommon and unfamiliar to the inexperienced control systems investigator. Two issues in particular are brought to mind: (1) the impact of performance on control systems when applying traditional IT security mitigation, and (2) the failure to spot significant cyber vulnerabilities that are not IP-related. The most likely way that cyber intrusions can be used to cause physical damage to equipment is not through the IP/Ethernet, but via non-wired approaches such as dial-up modems, direct connections to control networks by "foreign" laptops, and other similar means. Ideally, a team with both IT security and control systems expertise should perform control systems cyber vulnerability assessments.

## Control Systems Cyber Vulnerabilities

Electric utilities often require their vendors to supply the source code for SCADA/Energy Management System (EMS) applications. Utilities are also provided detailed technical manuals, training, and default passwords for vendor remote-access. There are only a limited number of SCADA/EMS suppliers and many are U.S. subsidiaries of foreign corporations with shared development in various European countries. The same systems installed in North American control centers are installed throughout the world, including in countries not necessarily friendly to the U.S. Consequently, utilities in

countries defined as “unfriendly” have a detailed understanding of the software and configuration of systems installed throughout North America.

Reliable operation of control systems depends on telecommunications including voice, data, radio, and microwave. In some cases, the telecommunications system is wholly under the ownership and operation of the utility. In other cases, telecommunication facilities are leased from telecommunication providers. These telecommunication providers have inadvertently contributed to control system unavailability (denial-of-service). For example, during the Slammer worm incident in 2003 the worm affected a telecommunication provider’s frame relay network, thereby preventing communications to and from a utility’s substation SCADA control system. In this case, the substation SCADA was effectively inoperable for approximately six to eight hours.

Currently, telecommunication vulnerabilities are not always addressed in control systems cyber security assessments or in programs including the NERC Cyber Security Standard-Urgent Action Standard 1200. Another example of how telecommunication vulnerabilities can impact control systems was revealed during an electric utility IT Telecom field audit of all phone lines in its operational facilities. The audit identified approximately 100 to 200 phone lines installed in power plants and substations that were not owned, or accounted for, by the utility. These phone lines were owned, installed, and paid for by the control and diagnostic systems’ suppliers, because the lines required modems for remote access to the control systems to meet warranty requirements. Since the phone lines belonged to the vendor and not the utility, the phone lines did not have the utility’s telephone prefix and were not identified in any war-dialing exercise. This is a common occurrence on many control system implementations throughout all critical industrial infrastructures.

Not being aware of phone lines installed in the field is one of many examples that can be cited in support of the need to benchmark the security status of facilities. This benchmarking process requires several activities:

- Performing vulnerability assessments to establish a baseline and then self-assessments to assure security is not being breached as systems are modified or changed. Detailed methodology needs to be developed.

- Performing a probabilistic risk assessment (PRA) of the vulnerability results to determine the level of mitigation required based on cost vs. risk. The PRA methodology has been used for commercial nuclear facilities, but will need to be adapted to meet control systems security applications. Additionally, training will be required for its implementation.

- Developing a detailed configuration management/configuration control program that identifies the current hardware, software, communication protocols, communication media, and patch level of control systems as-installed in the field.

- Developing detailed security policies and procedures specifically for control systems identifying activities that could compromise control systems security. This requires control systems, system operations, and IT security expertise.

Electronic vulnerabilities in operational systems are impacted by a variety of factors such as:

- Equipment suppliers provide remote dial-up access as part of their standard system configuration and utilize default passwords.

- Plant staff is reluctant to change default passwords because of personnel performance considerations during emergency events.

- Plant and corporate staff use remote desktop access software without adequate security considerations to manage and operate systems from off-site locations.

- Security patches often are not supplied to the end-users, or users are not applying the patches for fear of impacting system performance. Current practice is to apply the upgrades/patches after the PCS/SCADA vendors thoroughly test and validate patches, sometimes incurring a multiple-month delay in patch deployment.

- Most new control and diagnostic hardware and software are web-enabled or wireless, creating potential cyber vulnerabilities unless specifically addressed.

- Control systems networks utilize Internet-based control and diagnostic applications without IT Security's knowledge.

- Power marketers often feel they require immediate access to data generated by DCS and SCADA systems and often directly access these systems from the Internet to retrieve the data.

- Insecure tools such as ActiveX controls are packaged as part of the control system architecture.

- A common security recommendation for servers is to turn off or remove services that are not needed by the application (such as NETBIOS or Telnet). However, a pervasive problem with applications in general, and specifically with control systems, is that vendors do not document the services that are required for their software to properly function. They quite often install and turn on services that are not needed and use services known for their vulnerabilities when more secure alternatives are available (for example, Telnet vs. ssh-secure shell). This unnecessarily complicates the job of removing vulnerabilities and keeping systems patched and secure.

- Protocol analyzers are publicly available to translate and issue commands for control systems communication protocols making "security by obscurity" less relevant.

There have been numerous discussions and recommendations for preventing a recurrence of the August 14, 2003, Northeast Outage. In order to address reliability issues associated with the older electromechanical relays and switches, there has been a push to install new digital networked devices without necessarily addressing the newly created cyber vulnerabilities. Ergo, we are moving from a “cyber-dead” environment to a very “cyber-alive” environment that is more capable, extensible, and reliable, but also more vulnerable.

## The Threat

Cyber attacks on control systems can be targeted at specific systems, subsystems, and multiple locations simultaneously from remote locations. Such attacks can directly challenge equipment design and safety limits, potentially causing system malfunctions and shutdowns. Electronic attacks also can impact restoration efforts by manipulating procedures or dynamically changing equipment conditions.

### Actual Cases

Various cyber security intrusion studies by the Department of Energy and by commercial security consultants, including KEMA, have demonstrated the cyber vulnerabilities of control systems to unauthorized access. There have been more than forty real-world cases where control systems have been impacted by electronic means. These events have occurred in electric power control systems for transmission, distribution, generation (including fossil, gas turbine, and nuclear, where three plants experienced denial of service events), as well as control systems for water, oil/gas, chemicals, paper, and agri-businesses.

Some of these events have resulted in damage. Confirmed damage from cyber intrusions have included intentionally opening valves resulting in discharge of millions of liters of sewage, opening breaker switches, tampering with boiler control settings resulting in shutdown of utility boilers, shutdown of combustion turbine power plants, and shutdown of industrial facilities. However, none of these events have been identified in the traditional Internet monitoring organizations such as CERT/CC, SANS, or the Computer Security Institute-CSI. Additionally, none of the events and statistics quoted by these organizations specifically address control systems. As defined in the CERT for Control Systems (e-CERT) section below, this is a gap that needs to be addressed.

### Potential Scenario

There are many “doom and gloom” scenarios. I believe most cyber impacts will be minor in nature. However, very determined, knowledgeable attackers could potentially create long-term impacts on portions of the electric grid, especially when fed by single, critical substations. In May of last year, I developed a hypothetical scenario with input from several utility and DOE National Laboratory personnel on how, using only cyber, it would be possible to impact or shut down portions the electric grid for extended periods of time (e.g., from days to months). I presented this scenario at the May 2003 Georgia Tech Protective Relay Conference. The approximately 300 utility and vendor protective relay engineers concurred it was a plausible scenario. They only questioned impact duration, concluding that impact duration was a function of local redundancy, available spares, and backup capability.

### Market Issues

Control systems suppliers and diagnostic hardware and software system suppliers are responding to the market by supplying systems that are either Microsoft-based, web-based, and/or wireless enabled. Consequently, there may be inherent design and implementation of cyber vulnerabilities included in the products as delivered. Many vendors are not supplying secure control systems, perhaps because they feel there is no market for them. In addition, end-users are not specifying secure control systems in their purchase specifications since there is no mandate, nor do they want to spend the additional money it would take to develop a secure control system.

An additional issue is that there are no specifications to define a secure control system. Several groups including NIST's PCSRF and ISA's SP99 Committee are currently attempting to develop security specifications that end-users, system integrators, and control system vendors can reference.

## Securing Control Systems - What is Needed

Several key activities need to be addressed and require funding to secure control systems. It should be noted that control system cyber security improvements will have direct relevance to the entire industrial manufacturing enterprise in addition to the electric power industry.

### CERT for Control Systems - eCERT

I believe a primary reason why industry has been slow to respond to the issue of control system cyber security is the belief that vulnerabilities and risks are not real. I am not aware of a business case that has been developed for damage potential and associated costs. There has been almost no public identification of control systems intrusions, and therefore it has been difficult for companies to build a business case for more secure control systems.

Many groups manage and disseminate incident and vulnerability information for the Internet and other cyber-susceptible information systems. No one is providing this service for the PCS/SCADA environment on a consistent basis. As an example the CERT/CC at Carnegie-Mellon's Software Engineering Institute currently is not set up to monitor control systems intrusions or events. There is a need for industry-specific assessments and expertise to add credibility and value to the CERT process. Providing a service like a CERT for PCS/SCADA systems would have a far-ranging value and offer benefits across all utility and critical infrastructure industries.

An industry-wide CERT for Control Systems – "e-CERT" - could gather information from the various industries that use the same technology, making industry-specific Information Sharing and Analysis Centers (ISACs) more useful by providing information independent of any industry sector. Since the same PCS from vendor "X" is used in power, water, refineries, chemical plants, and paper mills, information on cyber vulnerabilities from any industry utilizing a PCS from vendor "X" would be of interest to all other industries (even if they are not considered critical infrastructures).

The e-CERT also could help dispel the various myths circulating that impede the awareness effort. I compiled one of the most comprehensive databases of control

systems impacts in the power industry in an informal and unstructured manner to begin this awareness process. As a result, DOE's Office of Energy Assurance (OEA) funded KEMA and Carnegie-Melon's Software Engineering Institute (CERT/CC) to prepare a scoping study for establishing the value of an energy-related CERT, e-CERT.

There is a need for a technical organization (such as CERT/CC) trusted by industry (vendors and end-users) that can gather sanitized information and have the technical expertise to analyze this information. I believe that the e-CERT concept could be one of the most valuable services the government can provide. It is anticipated that a steering group consisting of end-users, National Laboratories, and equipment suppliers would provide guidance on requirements, benefits, and process. The intent would be to have e-CERT analyze the information, work with the National Laboratories at the various SCADA and PCS test beds to determine the impacts, and then make that information available to the appropriate industry ISACs and relevant control systems user groups. The initial annual funding level would be on the order of $3 million, which seems a small price to pay to help secure the nation's critical infrastructures and the overall industrial manufacturing base.

## National SCADA Test Bed

To date, there has not been a concerted, independent effort to determine the exact vulnerabilities of control systems or the types of technology that should be employed to secure control systems. Rather, there has been an assumption that the encryption technology utilized to ensure confidentiality of data and communications over the Internet and traditional IT business systems will be sufficient for control systems. However, for control systems, confidentiality is not the primary security objective. For control systems, availability and message integrity are most critical, whereas confidentiality is secondary.

Most vulnerability assessments and intrusion testing of control systems in actual operation stop short of actually attempting to gain unauthorized access to the control systems. This is because the risk of interfering with the processes these systems control is too great.

Consequently, two critical areas need to be addressed to better secure control systems:

- Understand the damage that can be done if a control system is compromised, and

- Develop security technology specific to control systems that improves security without impacting the performance requirements.

The National SCADA Test Bed is in a unique position to meet these requirements. The Test Bed combines the best skills of the Idaho National Engineering and Environmental Laboratory (INEEL) and the Sandia National Laboratory (SNL) working together to secure critical infrastructure.

The large scale Test Bed is located at INEEL. INEEL has its own 138,000-volt grid independent of the local utility. This enables the Test Bed to test equipment in a representative environment. It also provides the capability to determine not only if a potential intruder can "touch" the control system and gain unauthorized access, but also

determine what damage can be done to the control system and the grid it is monitoring and controlling. The National SCADA Test Bed can, therefore, determine what mitigation technology needs to be developed. Additionally, the vulnerability assessments will be used as a starting point to develop security technologies specifically for control systems.

To date, several SCADA and other control systems vendors have provided control systems to the Test Bed. The National SCADA Test Bed is vendor independent and trusted by vendors and end-users. Consequently, the information from the Test Bed will be trusted by the industry, will allow off-line testing and validation of processes and procedures, will improve industry awareness, and will enable rapid dissemination of critical information (such as through e-CERT).

Another key function of the Test Bed will be its interaction with e-CERT. e-CERT, through its trusted relationships, could be the direct interface to industry in collecting and sorting vulnerability information and then performing preliminary assessments. That information will be supplied to the Test Bed for use in field-testing of actual control systems to confirm vulnerabilities and potential impacts. The Test Bed will then determine potential mitigation technology (hardware and/or guidelines) that can be disseminated through e-CERT, ISACs, and other avenues to the appropriate organizations.

Adequate funding is lacking to enable the Test Bed to function in a complete and timely manner. A significant multi-year investment is required.

## Summary/Conclusion

Control systems are different from traditional IT systems. The technology and information sharing necessary to secure these systems are not currently available. e-CERT and the National SCADA Test Bed can help strengthen the security of the control systems that are an integral part of the nation's critical infrastructure. A secondary benefit would be improved reliability and availability of the critical infrastructure services.

I am concerned that if we do not take these and more actions, the reliability and availability of our critical infrastructure will be vulnerable to intentional, or even unintentional, events in ways we have not contemplated.

Thank you Mr. Chairman, Committee Members, for your time and attention. I am happy to answer questions.

###

Joseph M. Weiss, P.E., C.I.S.M., is an Executive Consultant with KEMA Inc where he serves as a leading industry expert on control systems cyber security. He can be reached at jweiss@kemaconsulting.com.

KEMA Inc. is based in Burlington, Massachusetts with approximately 400 technical and management consulting specialists in offices throughout the United States and abroad. Assisting over 500 clients in more than 70 countries, KEMA provides technical and management consulting, testing, inspections, certification, and training services to utility and other process industries and end-users. More information on KEMA, Inc. can be found at www.kemainc.com.